

Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires

Marusia Rebolledo

15 octobre 2007

Résumé

We show how the formula of Gross and Kudla about triple product L -functions allows us to construct degree zero elements of the supersingular module annihilated by the winding ideal. Using the method of Parent, we apply those results to study rational points on modular curves : we determine a set of primes of analytic density $1 - 9/2^{10}$ for which the quotient of $X_0(p^r)$ ($r > 1$) by Atkin-Lehner operator w_{p^r} has no rational points other than the cusps and the CM points.

2000 Mathematics Subject Classification : Primary : 11G, 14G05 ; Secondary : 11R52

Introduction

Pour $N > 0$ un entier, notons $X_0(N)$ la courbe modulaire sur \mathbb{Q} classifiant grossièrement les courbes elliptiques généralisées munies d'une N -isogénie. La motivation initiale de ces travaux est l'étude des points rationnels du quotient $X_0^+(p^r)$ de $X_0(p^r)$ par l'involution d'Atkin-Lehner w_{p^r} pour p un nombre premier et $r > 1$ un entier. Pour cela, nous reprenons une méthode de Parent [21] s'inspirant des travaux de Momose [17, 18, 19] et faisant appel au *module supersingulier*.

Fixons $p > 3$ un nombre premier et $\overline{\mathbb{F}}_p$ une clôture algébrique de \mathbb{F}_p . Nous appelons *module supersingulier* le \mathbb{Z} -module libre \mathcal{P} engendré par l'ensemble fini $\mathcal{S} = \{x_0, \dots, x_g\}$ des classes d'isomorphismes de courbes elliptiques supersingulières sur $\overline{\mathbb{F}}_p$. Notons \mathcal{P}^0 le sous-groupe de \mathcal{P} constitué des éléments de degré nul. On peut munir \mathcal{P}^0 d'une action de l'anneau \mathbb{T} engendré par les opérateurs de Hecke agissant sur l'espace vectoriel $S_2(\Gamma_0(p))$ des formes paraboliques de poids 2 pour $\Gamma_0(p)$ (voir 1.1). Notons $\mathcal{P}^0[I_e]$ l'ensemble des éléments de \mathcal{P}^0 annulés par l'*idéal d'enroulement* $I_e \subset \mathbb{T}$ c'est-à-dire l'annulateur des formes primitives $f \in S_2(\Gamma_0(p))$ telles que $L(f, 1) \neq 0$. Pour $j \in \mathbb{P}^1(\overline{\mathbb{F}}_p)$ un invariant non supersingulier, considérons l'application

$$\iota_j : \begin{array}{ccc} \mathcal{P} & \longrightarrow & \overline{\mathbb{F}}_p \\ \sum_{i=0}^g \lambda_i x_i & \longmapsto & \sum_{i=0}^g \frac{\lambda_i}{j - j_i} \end{array} \quad (1)$$

où, pour $i \in \{0, \dots, g\}$, j_i est l'invariant d'une courbe elliptique $E_i \in x_i$. Parent a mis en évidence le critère suivant (voir propositions 3.1 et 3.2 de [21]) :

(C) *Soit $p \geq 11$. Supposons que pour tout $j \in \mathbb{F}_p$ non supersingulier, il existe $x \in \mathcal{P}^0[I_e]$ tel que $\iota_j(x) \neq 0$. Alors $X_0^+(p^r)(\mathbb{Q})$ est trivial c'est-à-dire ne contient que des pointes et des points CM.*

Pour A un anneau et $f : M \rightarrow N$ un homomorphisme de \mathbb{Z} -modules, on note $M_A = M \otimes A$ et on note encore $f : M_A \rightarrow N_A$ l'homomorphisme de A -modules obtenu par extension des scalaires. Soient n le numérateur de $(p-1)/12$ et $\pi^0 : \mathcal{P}_{\mathbb{Z}[1/n]} \rightarrow \mathcal{P}_{\mathbb{Z}[1/n]}^0$ la projection orthogonale (voir section 1.3). Pour $D > 0$ notons $\gamma_D \in \mathcal{P}_{\mathbb{Q}}$ le D -ième élément de Gross (voir 3.1). Notons $\text{Disc}(p)$ l'ensemble des discriminants quadratiques imaginaires¹ premiers à p . Parent déduit de la formule de Gross-Zhang que $\gamma_D^0 := \pi^0(\gamma_D) \in \mathcal{P}^0[I_e]_{\mathbb{Q}}$ pour $-D \in \text{Disc}(p)$. Considérons une autre famille d'éléments du module supersingulier :

$$y_m = \sum_{i=0}^g \left\langle T_m x_i, \frac{x_i}{w_i} \right\rangle x_i \in \mathcal{P} \quad \text{et} \quad y_m^0 = \pi^0(y_m) \in \mathcal{P}_{\mathbb{Z}[1/n]}^0 \quad (m \geq 1) \quad (2)$$

où $\langle \cdot, \cdot \rangle$ est l'accouplement bilinéaire sur \mathcal{P} défini en (3) et $w_i = |\text{Aut}(E_i)|/2$ pour $E_i \in x_i$.

Théorème 0.1 *Pour tout entier $m \geq 1$, $y_m^0 \in \mathcal{P}^0[I_e]_{\mathbb{Q}}$.*

Notons $a_E = \sum_{i=0}^g \frac{x_i}{w_i}$ l'élément d'Eisenstein (voir 1.3). L'assertion précédente peut se déduire de la formule de Gross-Kudla ou, pour certaines valeurs de m , de la formule de Gross-Zhang et de la proposition suivante

Proposition 0.1 *On a*

$$y_m = \epsilon(m) a_E + \sum_{\substack{(s,d) \in \mathbb{Z}^2 \\ 4m - s^2 = dr^2 > 0}} \gamma_d \quad (m \geq 1)$$

où $\epsilon(m) = 1$ si m est un carré et $\epsilon(m) = 0$ sinon.

La démonstration de la proposition 0.1 s'inspire du calcul classique qui permet d'établir la formule des traces d'Eichler (voir [7], [9] et la section 3.2).

Parent [21] montre que $\{\gamma_D^0, -D \in \text{Disc}(p)\}$ engendre le \mathbb{Q} -espace vectoriel $\mathcal{P}^0[I_e]_{\mathbb{Q}}$. Nous montrons au paragraphe 3.2 les propositions suivantes :

Proposition 0.2 *Le \mathbb{Q} -espace vectoriel engendré par $(y_m^0)_{m \geq 1}$ est égal au \mathbb{Q} -espace vectoriel engendré par $(y_m^0)_{1 \leq m \leq g+1}$.*

¹On appelle ici discriminant quadratique imaginaire le discriminant d'un ordre d'un corps quadratique imaginaire. C'est donc un carré mutlié par un discriminant fondamental.

Proposition 0.3 *Le $\mathbb{T}_{\mathbb{Q}}$ -module engendré par $\{y_m^0, m \geq 1\}$ est égal à $\mathcal{P}^0[I_e]_{\mathbb{Q}}$.*

Pour $-d < 0$ un discriminant fondamental, notons ε_d le caractère non trivial de $\text{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$. Les propositions 0.1, 0.2 et 0.3 entraînent une version précise d'un théorème de non-annulation :

Corollaire 0.1 *Si f est une forme primitive de poids 2 pour $\Gamma_0(p)$ telle que $L(f, 1) \neq 0$, alors il existe $d \leq 4g + 4$ tel que $L(f \otimes \varepsilon_d, 1) \neq 0$.*

Pour $(m, p) = 1$, y_m énumère les boucles du graphe des m -isogénies étudié par Mestre et Oesterlé [15]. Cela permet de faire les calculs section 4.2 conduisant au théorème 0.2 suivant.

Considérons le nombre premier $p_0 = 45321935159$. Soit \mathcal{C} l'ensemble des nombres premiers p qui sont un carré modulo 3, 4 et 7 et tels que l'une des conditions suivantes soit vérifiée :

1. p carré modulo 5, 11, 19, 23, 43, 67, 163, non carré modulo 8 ;
2. p carré modulo 8, 11, 19, et modulo au moins deux des nombres premiers 43, 67, 163, et vérifiant l'une des conditions suivantes
 - (a) p carré modulo 5 ;
 - (b) p non carré modulo 5 et 23 ;
 - (c) p non carré modulo 5 et carré modulo 23, 59, 71 ;
 - (d) p non carré modulo 5, 59, 71 et carré modulo 23 ;
3. p carré modulo 5, 8, 11, 43, 67, 163, non carré modulo 19 et l'une des conditions suivantes est vérifiée :
 - (a) p carré modulo 23 ;
 - (b) p non carré modulo 23 et $\left(\frac{p}{31}\right) \left(\frac{p}{36319}\right) \left(\frac{p}{p_0}\right) = 1$.
4. p carré modulo 5, 8, 19, 43, 67, 163, non carré modulo 11 et p carré modulo au moins un des nombres : 23, 797.

Théorème 0.2 *Si $p \geq 11$, $p \neq 13$ et $p \notin \mathcal{C}$, alors $X_0^+(p^r)(\mathbb{Q})$ est trivial.*

L'ensemble \mathcal{C} est de densité analytique $9/2^{10}$. Parent [21] avait obtenu un résultat analogue avec une densité de $7/2^9$. Le cas $r = 2$ de ce théorème constitue une avancée en direction du cas *normalisateur d'un Cartan déployé* d'un problème de Serre sur la torsion des courbes elliptiques². La liste des nombres premiers $11 \leq p \leq 50000$, $p \neq 13$ dans \mathcal{C} est donnée dans la table 5 page 15.

Remerciements. Je tiens ici à remercier L. Merel, P. Parent ainsi que le referee pour leurs remarques durant l'élaboration de cet article.

²Pour un énoncé de ce problème, se reporter à [24] ou [25] p. 288.

1 Préliminaires sur le module supersingulier

1.1 Réalisations géométriques et opérateurs de Hecke

Soit $\tilde{\mathbb{T}}$ l'anneau engendré par l'action des opérateurs de Hecke T_m , $m \geq 1$ sur le \mathbb{C} -espace vectoriel $M_2(\Gamma_0(p))$ des formes modulaires de poids 2 pour $\Gamma_0(p)$. Cette action se factorise par \mathbb{T} sur $S_2(\Gamma_0(p))$. Soient $X_0(p)_{\mathbb{Z}}$ la normalisation de $\mathbb{P}_{\mathbb{Z}}^1$ dans $X_0(p)$ via le morphisme composé $X_0(p) \rightarrow X_0(1) \cong \mathbb{P}_{\mathbb{Q}}^1$. La fibre $X_0(p)_{\mathbb{F}_p}$ de $X_0(p)_{\mathbb{Z}}$ en p est constituée de deux copies de $\mathbb{P}_{\mathbb{F}_p}^1$ qui sont échangées par l'opérateur d'Atkin-Lehner w_p et se coupent transversalement. Les points doubles de $X_0(p)_{\mathbb{F}_p}$ sont en correspondance bijective avec les classes x_0, \dots, x_g de \mathcal{S} et g n'est autre que le genre de $X_0(p)$. Notons $J_0(p)$ la jacobienne de $X_0(p)$ et \tilde{J} la jacobienne généralisée de $X_0(p)$ relativement aux pointes. L'anneau $\tilde{\mathbb{T}}$ (resp. \mathbb{T}) est isomorphe à l'anneau engendré par les endomorphismes de \tilde{J} (resp. $J_0(p)$) provenant des correspondances de Hecke sur $X_0(p)$. Soient $J_0(p)_{\mathbb{Z}}$ et $\tilde{J}_{\mathbb{Z}}$ les modèles de Néron respectifs de $J_0(p)$ et \tilde{J} sur \mathbb{Z} . Le groupe $\mathcal{P} = \mathbb{Z}[\mathcal{S}]$ (resp. \mathcal{P}^0) s'identifie au groupe des caractères de la composante neutre de la fibre en p de $\tilde{J}_{\mathbb{Z}}$ (resp. $J_0(p)_{\mathbb{Z}}$) (voir [22] et [6] 2.3). Cela définit par transport de structure une action de $\tilde{\mathbb{T}}$ sur \mathcal{P} qui laisse stable \mathcal{P}^0 et se factorise par \mathbb{T} sur \mathcal{P}^0 . L'action de $\tilde{\mathbb{T}}$ sur la classe d'isomorphisme $[E]$ d'une courbe elliptique E supersingulière sur \mathbb{F}_p est donnée par $T_m([E]) = \sum_C [E/C]$ ($m \geq 1$), où C parcourt l'ensemble des sous-schémas en groupes finis d'ordre m de E (voir [22] ou [15] 1.2.1). Sur la base $(x_i)_{0 \leq i \leq g}$ de \mathcal{P} , l'action de T_m ($m \geq 1$) est donnée par la transposée de la *matrice d'Eichler-Brandt* $B(m) = (B_{i,j}(m))_{0 \leq i,j \leq g}$ (voir [9] sections 1 et 4).

1.2 Accouplement bilinéaire

Soit δ le dénominateur de $(p-1)/12$. Rappelons que $w_i = |\text{Aut}(E_i)|/2$ ($i \in \{0, \dots, g\}$, $E_i \in x_i$) vérifie $\prod_{i=0}^g w_i = \delta$ et $\sum_{i=0}^g 1/w_i = (p-1)/12$.

Le \mathbb{Z} -module \mathcal{P} est muni de l'accouplement bilinéaire non dégénéré $\langle \cdot, \cdot \rangle : \mathcal{P} \times \mathcal{P} \rightarrow \mathbb{Z}$ défini par

$$\langle x_i, x_j \rangle = w_i \delta_{i,j} \quad (0 \leq i, j \leq g) \quad (3)$$

où $\delta_{i,j}$ est le symbole de Kronecker. Les opérateurs de Hecke sont auto-adjoints pour $\langle \cdot, \cdot \rangle$. Cet accouplement induit un homomorphisme injectif de $\tilde{\mathbb{T}}$ -modules de \mathcal{P} dans $\tilde{\mathcal{P}} = \text{Hom}(\mathcal{P}, \mathbb{Z})$ (sur lequel $\tilde{\mathbb{T}}$ agit par dualité) de conoyau isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$ identifiant $\tilde{\mathcal{P}}$ au sous- $\tilde{\mathbb{T}}$ -module $\bigoplus_{i=0}^g \mathbb{Z} \frac{x_i}{w_i}$ de $\mathcal{P}_{\mathbb{Q}}$ (voir [9] ou [8] lemme 3.16). L'accouplement canonique $\mathcal{P} \times \tilde{\mathcal{P}} \rightarrow \mathbb{Z}$ étend donc l'accouplement $\langle \cdot, \cdot \rangle$ et sera encore noté $\langle \cdot, \cdot \rangle$. L'homomorphisme injectif de \mathbb{T} -modules de \mathcal{P}^0 dans $\tilde{\mathcal{P}}^0 = \text{Hom}(\mathcal{P}^0, \mathbb{Z})$ induit par $\langle \cdot, \cdot \rangle$ est de conoyau isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (*loc. cit.*). Sur $\tilde{\mathcal{P}}^0/\mathcal{P}^0$ qui s'identifie au groupe des composantes de la fibre en p de $J_0(p)_{\mathbb{Z}}$, l'accouplement $\langle \cdot, \cdot \rangle$ n'est autre que l'accouplement de monodromie (voir [12] ou l'appendice de [3]).

Notons $\sum_{m \geq 0} a_m(f)q^m$ le développement de Fourier à l'infini de $f \in M_2(\Gamma_0(p))$. Considérons le \mathbb{Z} -module \mathcal{M} des formes modulaires f telles que $a_0(f) \in \mathbb{Q}$ et $a_m(f) \in \mathbb{Z}$ pour $m \geq 1$ et \mathcal{M}^0 le sous- \mathbb{Z} -module de \mathcal{M} constitué des formes paraboliques³. L'action de $\tilde{\mathbb{T}}$ sur $M_2(\Gamma_0(p))$ laisse stables \mathcal{M} et \mathcal{M}^0 et se factorise par \mathbb{T} sur \mathcal{M}^0 . On a $\mathcal{M}_{\mathbb{C}} = M_2(\Gamma_0(p))$ et $\mathcal{M}_{\mathbb{C}}^0 = S_2(\Gamma_0(p))$. L'accouplement sur $\mathcal{M} \times \tilde{\mathbb{T}}$ défini par $(f, T) \mapsto a_1(f | T)$ induit un isomorphisme de $\tilde{\mathbb{T}}$ -modules (resp. de \mathbb{T} -modules)

$$\mathcal{M} \xrightarrow{\sim} \text{Hom}(\tilde{\mathbb{T}}, \mathbb{Z}) \quad (\text{resp. } \mathcal{M}^0 \xrightarrow{\sim} \text{Hom}(\mathbb{T}, \mathbb{Z}))$$

(voir [23] théorème 2.2 et [8] proposition 1.3). Les homomorphismes de $\tilde{\mathbb{T}}$ -modules et \mathbb{T} -modules

$$\begin{aligned} \theta : \mathcal{P} \otimes_{\tilde{\mathbb{T}}} \tilde{\mathcal{P}} &\longrightarrow \text{Hom}(\tilde{\mathbb{T}}, \mathbb{Z}) \cong \mathcal{M} \\ x \otimes_{\tilde{\mathbb{T}}} y &\longmapsto \frac{1}{2}(\deg x \cdot \deg y) + \sum_{m \geq 1} \langle T_m x, y \rangle q^m \end{aligned}$$

et

$$\theta^0 : \mathcal{P}^0 \otimes_{\mathbb{T}} \tilde{\mathcal{P}}^0 \longrightarrow \text{Hom}(\mathbb{T}, \mathbb{Z}) \cong \mathcal{M}^0$$

qui se déduisent de l'accouplement $\langle \cdot, \cdot \rangle$, sont des surjections (voir [8] théorème 0.10).

1.3 Le $\tilde{\mathbb{T}}$ -module \mathcal{P}

Les $\tilde{\mathbb{T}}_{\mathbb{Q}}$ -modules $\mathcal{P}_{\mathbb{Q}}$ et $\mathcal{M}_{\mathbb{Q}}$ et les $\mathbb{T}_{\mathbb{Q}}$ -modules $\mathcal{P}_{\mathbb{Q}}^0$ et $\mathcal{M}_{\mathbb{Q}}^0$ sont libres de rang 1 (voir par exemple [9] et [16]). Appelons *forme de Hecke* une forme modulaire de poids 2 pour $\Gamma_0(p)$ propre pour tous les opérateurs de Hecke et normalisée, et *forme primitive* une forme de Hecke parabolique. On note Prim l'ensemble des formes primitives. Les idempotents primitifs de $\tilde{\mathbb{T}}_{\mathbb{Q}}$ sont en correspondance bijective avec les formes de Hecke et engendrent les sous- $\tilde{\mathbb{T}}_{\mathbb{Q}}$ -modules irréductibles de $\tilde{\mathbb{T}}_{\mathbb{Q}}$. On note $\mathbf{1}_f$ l'idempotent primitif associé à une forme de Hecke f . Les opérateurs de Hecke étant autoadjoints pour $\langle \cdot, \cdot \rangle$, le $\tilde{\mathbb{T}}_{\mathbb{Q}}$ -module $\mathcal{P}_{\mathbb{Q}}$ se décompose en somme directe de sous-espaces propres orthogonaux. Pour f une forme primitive, le sous-espace $\mathcal{P}_{\mathbb{Q}}^f = \mathbf{1}_f(\mathcal{P}_{\mathbb{Q}})$ est une \mathbb{Q} -droite dont on choisit un vecteur directeur a_f . Notons $\sigma'(m)$ la somme des diviseurs de m premiers à p . Le sous-espace propre associé à la série d'Eisenstein normalisée $E = \frac{p-1}{24} + \sum_{m \geq 1} \sigma'(m)q^m$ est engendré par l'*élément d'Eisenstein*

$$a_E = \sum_{i=0}^g \frac{x_i}{w_i} \in \tilde{\mathcal{P}} \subset \mathcal{P}_{\mathbb{Z}[1/\delta]}.$$

De plus, a_E vérifie $\langle x, a_E \rangle = \deg x$ ($x \in \mathcal{P}$). Par conséquent, $\mathcal{P}^E := \mathbb{Z} \cdot a_E$ est le \mathbb{Z} -module orthogonal à \mathcal{P}^0 pour $\langle \cdot, \cdot \rangle : \mathcal{P} \times \tilde{\mathcal{P}} \longrightarrow \mathbb{Z}$. On note

$$\begin{aligned} \pi^0 : \mathcal{P}_{\mathbb{Z}[1/n]} &\longrightarrow \mathcal{P}_{\mathbb{Z}[1/n]}^0 \\ x &\longmapsto x - \frac{12}{p-1} \deg(x) a_E \end{aligned}$$

la projection orthogonale.

³Pour $f \in \mathcal{M}$, on a en fait $\delta a_0(f) \in \mathbb{Z}$ (voir [8] proposition 1.1). Attention, les notations diffèrent de celles adoptées dans [8] où \mathcal{M} est noté \mathcal{N} .

1.4 Produits tensoriels

Considérons le $\tilde{\mathbb{T}}$ -module $\mathcal{P} \otimes_{\tilde{\mathbb{T}}} \mathcal{P}$. Les sous-espaces $\tilde{\mathbb{T}}_{\mathbb{Q}}$ -propres de $\mathcal{P}_{\mathbb{Q}} \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}$ sont les $\tilde{\mathbb{T}}_{\mathbb{Q}}$ -modules $\mathcal{P}_{\mathbb{Q}}^g \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^g$ pour g décrivant l'ensemble des formes de Hecke et on a les décompositions en sous-espaces deux à deux orthogonaux

$$\mathcal{P}_{\mathbb{Q}} \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}} = (\mathcal{P}_{\mathbb{Q}}^E \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^E) \oplus (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0) \quad \text{et} \quad \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0 = \bigoplus_{g \in \text{Prim}} (\mathcal{P}_{\mathbb{Q}}^g \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^g).$$

En effet, pour toutes formes de Hecke f, g et h , on a $\mathbf{1}_f (\mathcal{P}_{\mathbb{Q}}^g \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^h) \neq 0$ si et seulement si $f = g = h$. Donc si $g \neq h$, on a $\mathcal{P}_{\mathbb{Q}}^g \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^h = \sum_f \mathbf{1}_f (\mathcal{P}_{\mathbb{Q}}^g \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^h) = 0$.

Considérons à présent les $\tilde{\mathbb{T}}^{\otimes 3}$ -modules $\mathcal{P}^{\otimes 3}$, $\mathcal{M}^{\otimes 3}$, et les $\mathbb{T}^{\otimes 3}$ -modules $\mathcal{P}^{0 \otimes 3}$ et $\mathcal{M}^{0 \otimes 3}$. Par functorialité des algèbres tensorielles, on déduit de l'accouplement $\langle \cdot, \cdot \rangle$ un accouplement⁴ $\langle \cdot, \cdot \rangle^{\otimes 3} : \mathcal{P}^{\otimes 3} \times \mathcal{P}^{\otimes 3} \rightarrow \mathbb{Z}$. De même, le produit scalaire de Petersson (\cdot, \cdot) sur $\mathcal{M}_{\mathbb{C}}^0 \times \mathcal{M}_{\mathbb{C}}$ (normalisé comme dans [9] (7.1)) définit le produit scalaire de Petersson $(\cdot, \cdot)^{\otimes 3}$ sur $\mathcal{M}_{\mathbb{C}}^{0 \otimes 3} \times \mathcal{M}_{\mathbb{C}}^{\otimes 3}$ (normalisé par [10] (11.3)).

Les $\tilde{\mathbb{T}}_{\mathbb{Q}}^{\otimes 3}$ -modules $\mathcal{M}_{\mathbb{Q}}^{\otimes 3}$ et $\mathcal{P}_{\mathbb{Q}}^{\otimes 3}$ et les $\mathbb{T}_{\mathbb{Q}}^{\otimes 3}$ -modules $\mathcal{M}_{\mathbb{Q}}^{0 \otimes 3}$ et $\mathcal{P}_{\mathbb{Q}}^{0 \otimes 3}$ sont libres de rang 1. Les opérateurs de Hecke triples de $\tilde{\mathbb{T}}^{\otimes 3}$ sont autoadjoints pour $(\cdot, \cdot)^{\otimes 3}$ et $\langle \cdot, \cdot \rangle^{\otimes 3}$. Les idempotents primitifs de $\tilde{\mathbb{T}}_{\mathbb{Q}}^{\otimes 3}$ sont de la forme $\mathbf{1}_F = \mathbf{1}_{f_1} \otimes \mathbf{1}_{f_2} \otimes \mathbf{1}_{f_3}$ pour $F = f_1 \otimes f_2 \otimes f_3$ parcourant l'ensemble des formes de Hecke triples (c'est-à-dire telles que f_1, f_2 et f_3 soient des formes de Hecke). Le \mathbb{Q} -espace vectoriel $\mathcal{P}_{\mathbb{Q}}^F = \mathbf{1}_F \mathcal{P}_{\mathbb{Q}}^{\otimes 3}$ est une \mathbb{Q} -droite de vecteur directeur $A_F = a_{f_1} \otimes_{\mathbb{Q}} a_{f_2} \otimes_{\mathbb{Q}} a_{f_3}$. On a les décompositions en sous-espaces propres deux à deux orthogonaux

$$\mathcal{P}_{\mathbb{Q}}^{\otimes 3} = \bigoplus_F \mathcal{P}_{\mathbb{Q}}^F \quad \text{et} \quad (\mathcal{P}_{\mathbb{Q}}^0)^{\otimes 3} = \bigoplus_F \mathcal{P}_{\mathbb{Q}}^F,$$

la somme directe portant respectivement sur l'ensemble des formes de Hecke triples et l'ensemble des formes primitives triples. On vérifie aisément que pour toute forme de Hecke triple F , on a

$$\mathbf{1}_F X = \frac{\langle A_F, X \rangle^{\otimes 3}}{\langle A_F, A_F \rangle^{\otimes 3}} A_F \quad (X \in \mathcal{P}_{\mathbb{Q}}^{\otimes 3}). \quad (4)$$

2 Formule de Gross-Kudla et éléments de $\mathcal{P}^0[I_e]$

Soit

$$\Delta_3 = \sum_{i=0}^g \frac{1}{w_i} x_i^{\otimes 3} \in \mathcal{P}_{\mathbb{Q}}^{\otimes 3}$$

l'élément diagonal de Gross-Kudla. Posons $s : \mathcal{P} \otimes \mathcal{P} \rightarrow \mathcal{P} \otimes_{\tilde{\mathbb{T}}} \mathcal{P}$ la surjection canonique,

$$\bar{\Delta}_3 = (1 \otimes_{\mathbb{Q}} s)(\Delta_3) \in \mathcal{P}_{\mathbb{Q}} \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}} \otimes_{\tilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}})$$

⁴donné par $\langle a_1 \otimes a_2 \otimes a_3, b_1 \otimes b_2 \otimes b_3 \rangle^{\otimes 3} = \prod_{i=1}^3 \langle a_i, b_i \rangle$

et

$$\bar{\Delta}_3^0 = (\pi^0 \otimes_{\mathbb{Q}} s)(\Delta_3) = (\pi^0 \otimes_{\mathbb{Q}} 1)(\bar{\Delta}_3) \in \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}} \otimes_{\bar{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}).$$

Gross et Kudla [10] théorème 11.1 ont montré que pour F une forme primitive triple, on a

$$L(F, 2) = \frac{(F, F)^{\otimes 3}}{4\pi p} \langle \mathbf{1}_F \Delta_3, \mathbf{1}_F \Delta_3 \rangle^{\otimes 3}.$$

En particulier, lorsque $F = f \otimes h \otimes h$ ($f, h \in \text{Prim}$), par [10] (11.7), on obtient

$$L(f, 1)L(f \otimes \text{Sym}^2 h, 2) = \frac{(F, F)^{\otimes 3}}{4\pi p} \langle \mathbf{1}_F \Delta_3, \mathbf{1}_F \Delta_3 \rangle^{\otimes 3}. \quad (5)$$

Nous allons voir que cela entraîne le

Théorème 2.1 *On a*

$$\bar{\Delta}_3^0 = \bar{\Delta}_3 - \frac{12}{p-1} a_E \otimes_{\mathbb{Q}} \left(\sum_{i=0}^g x_i \otimes_{\bar{\mathbb{T}}_{\mathbb{Q}}} \frac{x_i}{w_i} \right)$$

et

$$\bar{\Delta}_3^0 \in \mathcal{P}^0[I_e]_{\mathbb{Q}} \otimes (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\bar{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0).$$

Remarque 1 Le \mathbb{T} -module \mathcal{P}^0 est localement libre après extension des scalaires à $\mathbb{Z}[1/2]$ (voir l'introduction de [8]), par conséquent il y a au pire de la 2-torsion dans $\mathcal{P}^0[I_e] \otimes (\mathcal{P}^0 \otimes_{\mathbb{T}} \mathcal{P}^0)$. Ainsi, puisque $\delta\Delta_3 \in \mathcal{P}^{\otimes 3}$, on a même $n\delta\bar{\Delta}_3^0 \in \mathcal{P}^0[I_e] \otimes (\mathcal{P}^0 \otimes_{\mathbb{T}} \mathcal{P}^0)$ à un élément de 2-torsion près.

Démonstration. – On a

$$\bar{\Delta}_3^0 = \sum_{i=0}^g \left(x_i - \frac{12}{p-1} a_E \right) \otimes_{\mathbb{Q}} \left(x_i \otimes_{\bar{\mathbb{T}}_{\mathbb{Q}}} \frac{x_i}{w_i} \right),$$

ce qui prouve la première assertion du théorème 2.1.

On a dans $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}} \otimes_{\bar{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}})$

$$\begin{aligned} \bar{\Delta}_3^0 &= \sum_{f, h \in \text{Prim}} (\mathbf{1}_f \otimes \mathbf{1}_h)(\bar{\Delta}_3) + \sum_{f \in \text{Prim}} (\mathbf{1}_f \otimes \mathbf{1}_E)(\bar{\Delta}_3) \\ &= (\mathbf{1} \otimes s) \left(\sum_{f, h \in \text{Prim}} (\mathbf{1}_f \otimes \mathbf{1}_h \otimes \mathbf{1}_h)(\Delta_3) + \sum_{f \in \text{Prim}} (\mathbf{1}_f \otimes \mathbf{1}_E \otimes \mathbf{1}_E)(\Delta_3) \right). \end{aligned}$$

Pour tout $f \in \text{Prim}$, on a (voir (4))

$$(\mathbf{1}_f \otimes \mathbf{1}_E \otimes \mathbf{1}_E)(\Delta_3) = \frac{\langle \Delta_3, a_f \otimes a_E \otimes a_E \rangle^{\otimes 3}}{\langle a_f \otimes a_E \otimes a_E, a_f \otimes a_E \otimes a_E \rangle^{\otimes 3}} (a_f \otimes a_E \otimes a_E).$$

Or $\langle \Delta_3, a_f \otimes a_E \otimes a_E \rangle^{\otimes 3} = \sum_{i=0}^g \frac{1}{w_i} \langle x_i, a_f \rangle \langle x_i, a_E \rangle^2 = \langle a_E, a_f \rangle = 0$. Par conséquent,

$$\begin{aligned} \bar{\Delta}_3^0 &= (1 \otimes s) \left(\sum_{f,h \in \text{Prim}} (\mathbf{1}_f \otimes \mathbf{1}_h \otimes \mathbf{1}_h)(\Delta_3) \right) \\ &= (1 \otimes s) \left(\sum_{\substack{f,h \in \text{Prim} \\ L(f,1) \neq 0}} (\mathbf{1}_f \otimes \mathbf{1}_h \otimes \mathbf{1}_h)(\Delta_3) + \sum_{\substack{f,h \in \text{Prim} \\ L(f,1) = 0}} (\mathbf{1}_f \otimes \mathbf{1}_h \otimes \mathbf{1}_h)(\Delta_3) \right). \end{aligned}$$

Puisque $(,)^{\otimes 3}$ et $\langle , \rangle^{\otimes 3}$ sont définis positifs, on déduit de (5) que lorsque $f \in \text{Prim}$ est telle que $L(f, 1) = 0$, alors $(\mathbf{1}_f \otimes \mathbf{1}_h \otimes \mathbf{1}_h)(\Delta_3) = 0$ ($h \in \text{Prim}$). Par ailleurs, rappelons que l'idéal I_e de \mathbb{T} est l'annulateur de l'ensemble des formes paraboliques f pour lesquelles $L(f, 1) \neq 0$ (voir [14]). On en déduit que, lorsque $f \in \text{Prim}$ est telle que $L(f, 1) \neq 0$, le vecteur propre associé a_f est dans $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ et donc $(\mathbf{1}_f \otimes \mathbf{1}_h \otimes \mathbf{1}_h)(\Delta_3) \in \mathcal{P}^0[I_e]_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}^0$ ($h \in \text{Prim}$). \square

On déduit immédiatement du théorème 2.1 le corollaire suivant :

Corollaire 2.1 *Pour toute forme \mathbb{Q} -linéaire ϕ sur $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$, on a $(1 \otimes_{\mathbb{Q}} \phi)(\bar{\Delta}_3^0) \in \mathcal{P}^0[I_e]_{\mathbb{Q}}$.*

Par définition de θ , on a

$$y_m = (1 \otimes (a_m \circ \theta))(\bar{\Delta}_3) \quad \text{et} \quad y_m^0 = (1 \otimes_{\mathbb{Q}} (a_m \circ \theta^0))(\bar{\Delta}_3^0). \quad (6)$$

Le théorème 0.1 énoncé dans l'introduction se déduit alors du corollaire 2.1 appliqué à $\phi = a_m \circ \theta^0$.

Remarque 2 Toute forme linéaire sur $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$ s'obtient comme combinaison linéaire des formes linéaires $a_m \circ \theta^0$ ($m \geq 1$) car $\theta^0 : \mathcal{P}_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0 \rightarrow \mathcal{M}_{\mathbb{Q}}^0$ est un isomorphisme. Il n'est donc pas restrictif de considérer les combinaisons linéaires d'éléments y_m^0 comme nous le faisons par la suite.

3 Les éléments y_m

3.1 Comparaison avec les éléments de Gross

Soit $D > 0$. Notons \mathcal{O}_{-D} l'ordre quadratique de discriminant $-D$ s'il existe et $u(-D)$ l'ordre de $\mathcal{O}_{-D}^*/\langle \pm 1 \rangle$. Pour $i \in \{0, \dots, g\}$, les anneaux $R_i = \text{End } E_i$, $i \in \{0, \dots, g\}$, sont des ordres maximaux de l'algèbre de quaternions \mathcal{B} sur \mathbb{Q} ramifiée en p et ∞ ; on note $h_i(-D)$ le nombre de plongements optimaux de \mathcal{O}_{-D} dans R_i modulo conjugaison par R_i^* . Le D -ième élément de Gross⁵ est défini par

$$\gamma_D = \frac{1}{2u(-D)} \sum_{i=0}^g h_i(-D) x_i \in \mathcal{P}_{\mathbb{Z}[1/6]}. \quad (7)$$

⁵Cet élément, introduit par Gross, est noté e_D dans [9] et [21].

On a $\gamma_D = 0$ si $-D$ n'est pas un discriminant quadratique imaginaire ou bien si p est décomposé dans $\mathbb{Q}(\sqrt{-D})$ (en effet, dans ce dernier cas, \mathcal{O}_{-D} ne se plonge pas dans l'algèbre de quaternions ramifiée en p et l'infini).

Démonstration de la proposition 0.1. – Soit $m \geq 1$ un entier. L'opérateur T_m agissant sur x_i par la transposée de la matrice de Brandt $B(m)$, on a $y_m = \sum_{i=0}^g B_{i,i}(m)x_i$. Notons N la norme réduite et tr la trace sur \mathcal{B} . On a

$$B_{i,i}(m) = \frac{1}{2w_i} \text{Card}\{b \in R_i ; N(b) = m\} = \frac{1}{2w_i} \sum_{\substack{s \in \mathbb{Z} \\ s^2 \leq 4m}} \text{Card}(A_i(s, m))$$

où

$$A_i(s, m) = \{b \in R_i ; N(b) = m, \text{tr}(b) = s\}.$$

Posons $D = 4m - s^2$. Lorsque $D = 0$, ce qui est possible si et seulement si m est un carré, $A_i(s, m)$ n'a qu'un seul élément. Considérons maintenant le cas où $D > 0$. Les éléments de $A_i(s, m)$ sont en bijection avec les plongements de \mathcal{O}_{-D} dans R_i . Pour chaque tel plongement f il existe un unique ordre \mathcal{O}_{-d} contenant \mathcal{O}_{-D} ($D = dr^2$ pour un certain r) tel que f s'étende en un plongement optimal de \mathcal{O}_{-d} dans R_i . On a donc une partition

$$A_i(s, m) = \bigsqcup_{\substack{d \in \mathbb{N}; \exists r \in \mathbb{N}; \\ dr^2 = D}} A_i(s, m)_d$$

où les éléments de $A_i(s, m)_d \subset A_i(s, m)$ correspondent aux plongements de \mathcal{O}_{-D} dans R_i qui s'étendent en un plongement optimal de \mathcal{O}_{-d} dans R_i . Comme

$$\text{Card}(A_i(s, m)_d) = h_i(-d) |R_i^\times / \mathcal{O}_{-d}^\times| = w_i h_i(-d) / u(-d),$$

on a finalement

$$\text{Card}(A_i(s, m)) = w_i \sum_{\substack{d \in \mathbb{N}; \exists r \in \mathbb{N}; \\ dr^2 = D}} \frac{h_i(-d)}{u(-d)}.$$

Par conséquent, pour tout entier $m > 0$, on a

$$\begin{aligned} y_m &= \sum_{4m=s^2} \sum_{i=0}^g \frac{x_i}{2w_i} + \sum_{i=0}^g \sum_{\substack{(s,d) \in \mathbb{Z} \times \mathbb{N} \\ \exists r > 0; 4m-s^2=dr^2 > 0}} \frac{h_i(-d)}{2u(-d)} x_i \\ &= \epsilon(m) a_E + \sum_{\substack{(s,d) \in \mathbb{Z} \times \mathbb{N} \\ 4m-s^2=dr^2 > 0}} \sum_{i=0}^g \frac{h_i(-d)}{2u(-d)} x_i. \end{aligned}$$

□

Remarque 3 Le raisonnement précédent est celui qui donne la formule d'Eichler pour la trace de T_m (voir [7] ou [9]). On retrouve cette formule en identifiant les degrés de chacun des membres de l'égalité de la proposition 0.1.

Remarque 4 La formule de Gross (voir [9] corollaire 11.6) montre que pour tout entier $d < 0$ premier à p , l'élément γ_d^0 est dans $\mathcal{P}^0[I_\epsilon]_{\mathbb{Q}}$ (voir par exemple [21]). La proposition 0.1 donne alors une nouvelle preuve du théorème 0.1 dans le cas particulier où m est tel que tout entier $d > 0$ tel que $4m - s^2 = dr^2$ soit premier à p .

La table 1 page 13 donne la décomposition de y_m comme combinaison linéaire d'éléments de Gross pour $m \leq 13$.

3.2 Espace vectoriel et module de Hecke engendrés par ces éléments

Nous démontrons dans ce paragraphe les propositions 0.2 et 0.3 ainsi que le corollaire 0.1. Faisons tout d'abord quelques observations. A une forme linéaire ϕ sur $\mathcal{P}_{\mathbb{Q}}$, associons la forme modulaire $\mathbf{g}_\phi = (\phi \otimes_{\mathbb{Q}} \theta^0)(\bar{\Delta}_3^0) \in \mathcal{M}_{\mathbb{Q}}^0$. Remarquons que \mathbf{g}_ϕ a pour q -développement

$$\sum_{m \geq 1} \phi(y_m^0) q^m. \quad (8)$$

De plus, puisque $\phi \otimes_{\mathbb{Q}} \theta^0$ est un homomorphisme de $\mathbb{T}_{\bar{\mathbb{Q}}} \otimes_{\bar{\mathbb{Q}}} \mathbb{T}_{\bar{\mathbb{Q}}}$ -modules, on a

$$\mathbf{1}_h \mathbf{g}_\phi = (\phi \otimes_{\mathbb{Q}} \theta^0) \left(\sum_{g \in \text{Prim}} (\mathbf{1}_g \otimes_{\bar{\mathbb{Q}}} \mathbf{1}_h)(\bar{\Delta}_3) \right) \quad (h \in \text{Prim}). \quad (9)$$

Démonstration de la proposition 0.2 Il suffit de montrer que toute forme linéaire sur l'espace vectoriel engendré par $(y_m^0)_{m \geq 1}$ et qui s'annule en y_1^0, \dots, y_{g+1}^0 est nulle. Soit ϕ une telle forme linéaire. La forme différentielle ω_ϕ de $X_0(p)$ associée à \mathbf{g}_ϕ a pour q -développement

$$\sum_{m \geq 1} \phi(y_m^0) q^m \frac{dq}{q}.$$

Si $\phi(y_1^0) = 0, \dots, \phi(y_{g+1}^0) = 0$, la forme différentielle holomorphe ω_ϕ a un zéro d'ordre g en l'infini. L'infini n'étant pas un point de Weierstrass de $X_0(p)$ (voir [20]), on en déduit que ω_ϕ est nulle, d'où la proposition.

Démonstration de la proposition 0.3

Lemme 3.1 Soient f et h deux formes primitives. Les assertions suivantes sont équivalentes :

$$a) L(f, 1)L(f \otimes \text{Sym}^2 h, 2) = 0 ; \quad b) \mathbf{1}_h \cdot \mathbf{g}_{\langle \cdot, a_f \rangle} = 0.$$

Démonstration. - D'après (9), on a

$$\mathbf{1}_h \mathbf{g}_{\langle \cdot, a_f \rangle} = (\langle \cdot, a_f \rangle \otimes_{\bar{\mathbb{Q}}} \theta^0) \left(\sum_{g \in \text{Prim}} (\mathbf{1}_g \otimes_{\bar{\mathbb{Q}}} \mathbf{1}_h)(\bar{\Delta}_3) \right).$$

Puisque $\langle a_g, a_f \rangle = 0$ si $g \neq f$, on obtient

$$\mathbf{1}_h \mathbf{g}_{\langle \cdot, a_f \rangle} = (\langle \cdot, a_f \rangle \otimes_{\mathbb{Q}} \theta^0)(\mathbf{1}_f \otimes_{\mathbb{Q}} \mathbf{1}_h)(\bar{\Delta}_3).$$

Or l'application

$$\langle \cdot, a_f \rangle \otimes_{\mathbb{Q}} \theta^0 : \mathcal{P}_{\mathbb{Q}}^f \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0) \longrightarrow \mathcal{M}_{\mathbb{Q}}^0$$

est injective car θ^0 est un isomorphisme de $\mathbb{T}_{\mathbb{Q}}$ -modules libres (voir fin de la section 1.1). Par conséquent $\mathbf{1}_h \mathbf{g}_{\langle \cdot, a_f \rangle} = 0$ si et seulement si $(\mathbf{1}_f \otimes_{\mathbb{Q}} \mathbf{1}_h)(\bar{\Delta}_3) = 0$ i.e. si et seulement si $(\mathbf{1}_f \otimes_{\mathbb{Q}} \mathbf{1}_h \otimes_{\mathbb{Q}} \mathbf{1}_h)(\Delta_3) = 0$. D'après (5), ceci est équivalent à l'assertion a). \square

Lemme 3.2 *Les conditions suivantes sont équivalentes :*

- i) le $\mathbb{T}_{\mathbb{Q}}$ -module \mathcal{Y} engendré par $\{y_m^0, m \geq 1\}$ est égal à $\mathcal{P}^0[I_e]_{\mathbb{Q}}$;
- ii) pour toute forme primitive f de poids 2 pour $\Gamma_0(p)$ telle que $L(f, 1) \neq 0$, il existe une forme primitive h de poids 2 pour $\Gamma_0(p)$ telle que $L(f \otimes \text{Sym}^2 h, 2) \neq 0$.

Démonstration. – Les espaces $\mathbb{T}_{\mathbb{Q}}$ -propres de $\mathcal{P}_{\mathbb{Q}}^0$ étant des \mathbb{Q} -droites, on a $\mathcal{Y} = \mathcal{P}^0[I_e]_{\mathbb{Q}}$ si et seulement si pour tout $f \in \text{Prim}$ tel que $L(f, 1) \neq 0$, il existe $m \geq 1$ tel que $\mathbf{1}_f y_m \neq 0$. Par ailleurs, d'après le lemme 3.1, la condition ii) du lemme est vérifiée si et seulement si pour tout $f \in \text{Prim}$ tel que $L(f, 1) \neq 0$, on a $\mathbf{g}_{\langle \cdot, a_f \rangle} \neq 0$ (car il existe alors h telle que $\mathbf{1}_h \mathbf{g}_{\langle \cdot, a_f \rangle} \neq 0$). Puisque $\mathbf{g}_{\langle \cdot, a_f \rangle}$ a pour q -développement $\sum_{m \geq 1} \langle y_m, a_f \rangle q^m$ (voir (8)), on en déduit l'équivalence des assertions i) et ii). \square

D'après les travaux de Schulze-Pillot et Böcherer [4] améliorés par Arakawa et Böcherer [1], la condition ii) du lemme ci-dessus est toujours satisfaite (voir [1] théorème 5.3). Cela prouve la proposition 0.3.

Démonstration du corollaire 0.1 Soit $f \in \text{Prim}$ telle que $L(f, 1) \neq 0$. D'après les propositions 0.2 et 0.3, il existe alors $1 \leq m \leq g + 1$ tel que $\mathbf{1}_f y_m \neq 0$. Par conséquent, il existe $D \leq 4g + 4$ tel que $\mathbf{1}_f \gamma_D \neq 0$. On a $(D, p) = 1$ car $D \leq 4g + 4$. Soit $-d$ le discriminant fondamental de $\mathbb{Q}(\sqrt{-D})$. En vertu des *relations de norme* [2] 2.4, on a $\gamma_D \in \tilde{\mathbb{T}} \cdot \gamma_d$. On en déduit que $\mathbf{1}_f \gamma_d \neq 0$ et $L(f \otimes \varepsilon_d, 1) \neq 0$ d'après la formule de Gross [9] corollaire 11.6 généralisée par Zhang [27] théorème 1.3.2.

4 Points rationnels de courbes modulaires

4.1 Une question théorique

On suppose désormais $p \geq 11$. Soit $\mathbb{Z}_{(p)}$ le localisé de \mathbb{Z} en p . Soit $j \in \mathbb{P}^1(\bar{\mathbb{F}}_p)$ non supersingulier. On étend ι_j à $\mathcal{P}_{\mathbb{Z}_{(p)}}$ en posant $\iota_j(1/a) = a^{-1}$. Supposons vérifiée la condition :

- (H) Pour tout $j \in \mathbb{F}_p$ ordinaire, il existe $m \geq 1$ tel que $\iota_j(y_m^0) \neq 0$.

D'après le théorème 0.1 et le critère (C) énoncé dans l'introduction, on a alors $X_0^+(p^r)(\mathbb{Q})$ trivial. Actuellement, on ne sait pas si pour p assez grand (par exemple $p > 37$), l'hypothèse (H) est vérifiée. Dans l'espoir d'obtenir un résultat sans les contraintes de congruence du théorème 0.2, remarquons que l'on peut reformuler cette condition. On a $(1 \otimes \theta^0)(\bar{\Delta}_3^0) \in \mathcal{P}_{\mathbb{Z}[1/n]}^0 \otimes \mathcal{M}^0$. Considérons la forme parabolique à coefficients dans $\bar{\mathbb{F}}_p$ (i.e. l'élément de $\bar{\mathbb{F}}_p \otimes \mathcal{M}^0$) définie par

$$\mathbf{g}_j = (\iota_j \otimes \theta^0)(\bar{\Delta}_3^0) \in \mathcal{M}_{\bar{\mathbb{F}}_p}^0. \quad (10)$$

Cette forme modulaire a pour q -développement $\sum_{m \geq 1} \iota_j(y_m^0) q^m$. L'hypothèse (H) est donc équivalente à :

$$(H') \quad \text{Pour tout } j \in \mathbb{F}_p \text{ ordinaire, on a } \mathbf{g}_j \neq 0.$$

4.2 Calculs pratiques : démonstration du théorème 0.2

Soit $j \in \mathbb{F}_p$ non supersingulier. On a

$$\iota_j(y_m^0) = \sum_{i=0}^g \frac{B_{i,i}(m)}{j - j_i} + 12 \operatorname{tr}(B(m)) \sum_{i=0}^g \frac{1}{w_i(j - j_i)} \in \bar{\mathbb{F}}_p.$$

En effet, $y_m^0 = y_m - \frac{12}{p-1} \deg(y_m) a_E$ et $\iota_j(a_E) = \sum_{i=0}^g \frac{1}{w_i(j - j_i)}$.

Le terme $\sum_{i=0}^g \frac{1}{w_i(j - j_i)}$ n'étant pas facile à calculer, nous introduisons

$$y_{k,m} = \operatorname{tr} B(m) y_k - \operatorname{tr} B(k) y_m \in \mathcal{P}^0[I_e]_{\mathbb{Q}} \quad (0 < k < m)$$

et calculons $\iota_j(y_{k,m})$ pour k, m dans $\{2, 3, 5, 6, 7\}$.

Lorsque $(m, p) = 1$, l'entier $B_{i,i}(m)$ est la multiplicité de j_i comme racine du polynôme modulaire $\phi_m(X, X)$ dans $\bar{\mathbb{F}}_p$ (voir [11] ou [13] 5.3 théorème 5). Les polynômes $\phi_m(X, X)$ pour $m \in \{2, 3, 5, 6, 7\}$, donnés par [26], sont énumérés dans la table 2 page 14. Comme m n'est pas carré, les racines de $\phi_m(X, X)$ dans \mathbb{C} sont les invariants $j(\tau)$ de courbes elliptiques à multiplication complexe par un ordre quadratique imaginaire $\mathbb{Z}[\tau]$. Les ordres quadratiques associés aux invariants racines des facteurs de degré 1 sont donnés dans la littérature (voir par exemple [5] 7.2.3). En déterminant les ordres quadratiques imaginaires possédant un élément de norme 5, 6 et 7, on trouve une racine α_i du facteur P_i de degré 2 pour $i \in \{1, \dots, 4\}$ (voir tables 2 et 3). On obtient ainsi les valeurs de $B_{i,i}(m)$ ($m \in \{2, 3, 5, 6, 7\}$) données dans la table 3 où $a, b, c, d, e, f, g, h, v, w \in \{0, 1\}$ sont par définition égaux à 1 si et seulement si $j(\tau)$ est supersingulier modulo p c'est-à-dire si p est inerte ou ramifié dans $\mathbb{Q}(\tau)$.

On supposera désormais que $p > 173$. Dans ce cas, les invariants apparaissant dans cette table sont tous distincts.

On a $a = c$ équivaut à $h = d$ et $a = d$ équivaut à $v = g$. On fait parcourir au 8-uplet (a, b, c, d, e, f, g, w) les différentes valeurs possibles. Pour (a, b, c, d, e, f, g, w) distincts des 8-uplets énumérés dans la table 4 page 15, les fractions $\iota_j(y_{k,m})$, $k, m \in \{2, 3, 5, 6, 7\}$, ne s'annulent pas simultanément. La table résume les résultats obtenus pour les 8-uplets posant un problème. Lorsque $\iota_j(y_{k,m})$ n'est pas une fraction identiquement nulle, on note $n_{k,m}$ le degré de son numérateur. Lorsque $n_{k,m} = 2$, $\iota_j(y_{k,m})$

a un zéro dans \mathbb{F}_p si et seulement si le discriminant $d_{k,m}$ de son numérateur (dans \mathbb{Z}) est un carré modulo p .

À titre d'exemple, lorsque $(a, b, c, d, e, f, g, w) = (0, 0, 1, 0, 0, 0, 0, 0)$, on obtient

$$\iota_j(y_{2,3}) = \iota_j(y_{2,5}) = \iota_j(y_{3,5}) = \iota_j(y_{5,6}) = \iota_j(y_{5,7}) = 0$$

et $\iota_j(y_{2,6})$, $\iota_j(y_{3,6})$, $\iota_j(y_{2,7})$, $\iota_j(y_{3,7})$ et $\iota_j(y_{6,7})$ sont, à multiplication par une puissance de 2 près, égaux à

$$Q(j) = \frac{2}{j - 8000} - \frac{P'_2(j)}{P_2(j)} = \frac{-2^{11} (13.181 j + 2^6 .3^3 .7.13.29)}{(j - 8000)P_2(j)}$$

qui s'annule en $j_0 \equiv -(181)^{-1} .2^6 .3^3 .7.29 \pmod{p}$.

Posons \mathcal{B} l'ensemble des nombres premiers p qui sont simultanément un carré modulo 3, 4 et 7 et qui vérifient l'une des conditions suivantes :

- i) p carré modulo 5, 11, 19, et 23 et non carré modulo 8,
- ii) p est un carré modulo 5, 8, 11 et 19;
- iii) p carré modulo 8, 11 et 19, non carré modulo 5, 23;
- iv) p carré modulo 8, 11, 19, 23, 59, 71, non carré modulo 5;
- v) p carré modulo 8, 11, 19, 23, non carré modulo 5, 59, 71;
- vi) p carré modulo 5, 8, 11, 23, non carré modulo 19;
- vii) p carré modulo 5, 8, 11, non carré modulo 19, 23 et $\left(\frac{p}{31}\right) \left(\frac{p}{36319}\right) \left(\frac{p}{p_0}\right) = 1$;
- viii) p carré modulo 5, 8, 19, 23, non carré modulo 11;
- ix) p carré modulo 5, 8, 19, 797, non carré modulo 11, 23.

Lemme 4.1 *Si $p > 173$, $p \neq 797, 36319, p_0$ et $p \notin \mathcal{B}$, alors pour tout $j \in \mathbb{F}_p$ non supersingulier, il existe $(k, m) \in \{2, 3, 5, 6, 7\}^2$ tel que $\iota_j(y_{k,m}) \neq 0$ et par conséquent $X_0^+(p^r)(\mathbb{Q})$ est trivial.*

Démonstration. – On vérifie aisément que lorsque p est comme dans l'énoncé et $j \in \mathbb{F}_p$, nous ne sommes pas dans l'un des cas énumérés dans la table 4 et donc il y a une fraction non nulle parmi $\iota_j(y_{k,m})$, $(k, m) \in \{2, 3, 5, 6, 7\}^2$.
□

Le lemme 4.1 et le théorème 1.1 de [21] entraînent alors le théorème 0.2. En effet, l'ensemble \mathcal{C} du théorème 0.2 est égal à $\mathcal{A} \cap \mathcal{B}$ et $797, 36319, p_0$ ne sont pas dans \mathcal{A} (ici \mathcal{A} est l'ensemble du théorème 1.1 de [21]). Le cas des nombres premiers $11 \leq p \leq 173, p \neq 13$ a été traité par [21] (voir la preuve du théorème 1.1 p. 8).

5 Tables

Table 1 Décomposition de y_m , $m \leq 13$ comme combinaison linéaire d'éléments de Gross.

$$\begin{aligned}
y_1 &= a_E + 2\gamma_3 + \gamma_4 \\
y_2 &= 2\gamma_4 + 2\gamma_7 + \gamma_8 \\
y_3 &= 3\gamma_3 + 2\gamma_8 + 2\gamma_{11} + \gamma_{12} \\
y_4 &= a_E + 2\gamma_3 + \gamma_4 + 2\gamma_7 + 2\gamma_{12} + 2\gamma_{15} + \gamma_{16} \\
y_5 &= 4\gamma_4 + 2\gamma_{11} + 2\gamma_{16} + 2\gamma_{19} + \gamma_{20} \\
y_6 &= 2\gamma_8 + 2\gamma_{15} + 2\gamma_{20} + 2\gamma_{23} + \gamma_{24} \\
y_7 &= 6\gamma_3 + \gamma_7 + 2\gamma_{12} + 2\gamma_{19} + 2\gamma_{24} + 2\gamma_{27} + \gamma_{28} \\
y_8 &= 2\gamma_4 + 4\gamma_7 + \gamma_8 + 2\gamma_{16} + 2\gamma_{23} + 2\gamma_{28} + 2\gamma_{31} + \gamma_{32} \\
y_9 &= a_E + 2\gamma_3 + \gamma_4 + 2\gamma_8 + 2\gamma_{11} + 2\gamma_{20} + 2\gamma_{27} + 2\gamma_{32} + 2\gamma_{35} + \gamma_{36} \\
y_{10} &= 4\gamma_4 + 2\gamma_{15} + 2\gamma_{24} + 2\gamma_{31} + 2\gamma_{36} + 2\gamma_{39} + \gamma_{40} \\
y_{11} &= 2\gamma_7 + 2\gamma_8 + \gamma_{11} + 2\gamma_{19} + 2\gamma_{28} + 2\gamma_{35} + 2\gamma_{40} + 2\gamma_{43} + \gamma_{44} \\
y_{12} &= 3\gamma_3 + 2\gamma_8 + 2\gamma_{11} + 3\gamma_{12} + 2\gamma_{23} + 2\gamma_{32} + 2\gamma_{39} + 2\gamma_{44} + 2\gamma_{47} + \gamma_{48} \\
y_{13} &= 6\gamma_3 + 4\gamma_4 + 2\gamma_{12} + 2\gamma_{16} + 2\gamma_{27} + 2\gamma_{36} + 2\gamma_{43} + 2\gamma_{48} + 2\gamma_{51} + \gamma_{52}.
\end{aligned}$$

Table 2 Polynômes modulaires ϕ_m , $m \in \{2, 3, 5, 6, 7\}$.

$$\begin{aligned}
\phi_2(X, X) &= -(X - 1\,728)(X + 3\,375)^2(X - 8\,000) \\
\phi_3(X, X) &= -X(X - 54\,000)(X + 32\,768)^2(X - 8\,000)^2 \\
\phi_5(X, X) &= -(X - 1\,728)^2(X - 287\,496)^2(X + 32\,768)^2(X + 884\,736)^2 P_1 \\
\phi_6(X, X) &= (X - 8\,000)^2 P_1^2 P_2 P_3^2 P_4^2 \\
\phi_7(X, X) &= -(X + 3\,375)(X - 16\,581\,375)X^2(X - 54\,000)^2 \\
&\quad \times (X + 12\,288\,000)^2(X + 884\,736)^2 P_2^2
\end{aligned}$$

où

$$\begin{aligned}
P_1 &= X^2 - 1\,264\,000 X - 681\,472\,000 \\
P_2 &= X^2 - 4\,834\,944 X + 14\,670\,139\,392 \\
P_3 &= X^2 + 191\,025 X - 121\,287\,375 \\
P_4 &= X^3 + 3\,491\,750 X^2 - 5\,151\,296\,875 X + 12\,771\,880\,859\,375
\end{aligned}$$

Table 3 Valeurs de $B_i(m) = B_{i,i}(m)$, $m \in \{2, 3, 5, 6, 7\}$.

j_i	τ	D_τ		$B_i(2)$	$B_i(3)$	$B_i(5)$	$B_i(6)$	$B_i(7)$
1728	$\sqrt{-1}$	4	a	1		2		
287496	$2\sqrt{-1}$	4	a			2		
-3375	$(1 + \sqrt{-7})/2$	7	b	2				1
16581375	$\sqrt{-7}$	7	b					1
8000	$\sqrt{-2}$	8	c	1	2		2	
0	$(1 + \sqrt{-3})/2$	3	d		1			2
54000	$\sqrt{-3}$	3	d		1			2
-12288000	$(1 + 3\sqrt{-3})/2$	3	d					2
-32768	$(1 + \sqrt{-11})/2$	11	e		2	2		
-884736	$(1 + \sqrt{-19})/2$	19	f			2		2
α_1	$\sqrt{-5}$	20	g			1	2	
α_2	$\sqrt{-6}$	24	h				1	2
α_3	$(1 + \sqrt{-15})/2$	15	v				2	
α_4	$(1 + \sqrt{-23})/2$	23	w				2	

Table 4 Résultats des calculs.

- $(a, b, c, d, e, f, g, w) = (0, 0, 1, 0, 0, 0, 0, 0)$: voir exemple dans le texte.
- $(a, b, c, d) = (0, 0, 0, 0)$ et

e	f	g	w	Résultat
0	0	*		$\iota_j(y_{k,m}) = 0$ ($k, m \in \{2, 3, 5, 6, 7\}$)
		1	0	$n_{5,6} = 2$, $d_{5,6} = 2^6 \cdot 5^6 \cdot 11^5 \cdot 13^4 \cdot 37^2 \cdot 59 \cdot 71$, $\iota_j(y_{k,m}) = 0$ ($k, m \neq (5, 6)$)
		1	1	$n_{5,6} = 5$, $\iota_j(y_{k,m}) = 0$ ($k, m \neq (5, 6)$)
0	1	0	0	$\iota_j(y_{k,m}) = 0$ ($k, m \in \{2, 3, 5, 6, 7\}$)
		0	1	$\iota_j(y_{5,6}) = \iota_j(y_{6,7})$, $n_{5,6} = 2$, $d_{5,6} = 2^6 \cdot 5^7 \cdot 7^4 \cdot 31 \cdot 36319 \cdot p_0$ $\iota_j(y_{k,m}) = 0$ ($k, m \neq (5, 6), (6, 7)$)
1	0	0	0	$\iota_j(y_{k,m}) = 0$ ($k, m \in \{2, 3, 5, 6, 7\}$)
		0	1	$\iota_j(y_{3,6}) = \iota_j(y_{5,6})$, $n_{5,6} = 2$, $d_{5,6} = 2^6 \cdot 3 \cdot 5^7 \cdot 7^8 \cdot 11^2 \cdot 17^2 \cdot 19^2 \cdot 797$ $\iota_j(y_{k,m}) = 0$ ($k, m \neq (3, 6), (5, 6)$)

Le symbole * signifie que le coefficient peut prendre indifféremment la valeur 0 ou 1. On rappelle que $p_0 = 45321935159$.

Table 5 Nombres premiers $p \leq 50000$ dans l'ensemble \mathcal{C} .

1873	3217	7417	8233	9241	10333	11257
15733	16921	17389	18313	19273	21961	26161
26497	26833	30097	31081	32377	34057	35281
36793	38329	38833	41617	42337	42793	48409

Références

- [1] T. Arakawa and S. Böcherer. Vanishing of certain spaces of elliptic modular forms and some applications. *J. Reine Angew. Math.*, 559 :25–51, 2003.

- [2] M. Bertolini and H. Darmon. Heegner points on Mumford-Tate curves. *Invent. Math.*, 126(1) :413–456, 1996.
- [3] M. Bertolini and H. Darmon. A rigid analytic Gross-Zagier formula and arithmetic applications. *Ann. of Math. (2)*, 146(1) :111–147, 1997. With an appendix by Bas Edixhoven.
- [4] S. Böcherer and R. Schulze-Pillot. Squares of automorphic forms on quaternion algebras and central values of L -functions of modular forms. *J. Number Theory*, 76(2) :194–205, 1999.
- [5] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [6] E. de Shalit. On certain Galois representations related to the modular curve $X_1(p)$. *Compositio Math.*, 95(1) :69–100, 1995.
- [7] M. Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.*, 195 :127–151 (1956), 1955.
- [8] M. Emerton. Supersingular elliptic curves, theta series and weight two modular forms. *J. Amer. Math. Soc.*, 15(3) :671–714 (electronic), 2002.
- [9] B. H. Gross. Heights and the special values of L -series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.
- [10] B. H. Gross and S. S. Kudla. Heights and the central critical values of triple product L -functions. *Compositio Math.*, 81(2) :143–209, 1992.
- [11] J. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81 :561–577, 1959.
- [12] L. Illusie. Réalisation l -adique de l'accouplement de monodromie d'après A. Grothendieck. *Astérisque*, (196-197) :7, 27–44 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).
- [13] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.
- [14] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3) :437–449, 1996.
- [15] J.-F. Mestre and J. Oesterlé. Courbes elliptiques de conducteur premier. non publié.
- [16] T. Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.
- [17] F. Momose. Rational points on the modular curves $X_{\text{split}}(p)$. *Compositio Math.*, 52(1) :115–137, 1984.
- [18] F. Momose. Rational points on the modular curves $X_0^+(p^r)$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 33(3) :441–466, 1986.
- [19] F. Momose. Rational points on the modular curves $X_0^+(N)$. *J. Math. Soc. Japan*, 39(2) :269–286, 1987.
- [20] A. P. Ogg. On the Weierstrass points of $X_0(N)$. *Illinois J. Math.*, (29) :31–35, 1978.

- [21] P. Parent. Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$. *Compos. Math.*, 141(3) :561–572, 2005.
- [22] M. Raynaud. Jacobienne des courbes modulaires et opérateurs de Hecke. *Astérisque*, (196-197) :9–25 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).
- [23] K. A. Ribet. Mod p Hecke operators and congruences between modular forms. *Invent. Math.*, 71(1) :193–205, 1983.
- [24] J.-P. Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4) :259–331, 1972.
- [25] J.-P. Serre. *Œuvres. Vol. III*. Springer-Verlag, Berlin, 1986. 1972–1984.
- [26] Magma Computational Algebra System. Available from <http://magma.maths.usyd.edu.au/magma/>.
- [27] S.-W. Zhang. Gross-Zagier formula for GL_2 . *Asian J. Math.*, 5(2) :183–290, 2001.

Marusia REBOLLEDO
 Laboratoire de Mathématiques
 Université Blaise Pascal
 Campus Universitaire des Cézeaux
 63177 Aubière cedex
 France